CTED
Counter-Terrorism Committee
Executive Directorate

ICT for peace foundation

UNCTED-ICT4Peace Foundation

Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes

Zurich Workshop, 25 August 2016

Summary Report

sponsored by

the Governments of Switzerland and Spain

and

Microsoft facebook KASPERSKY lab

CTED
Counter-Terrorism Committee
Executive Directorate

ICT for peace foundation

TABLE OF CONTENTS

BACKGROUND 3

SUMMARY OF WORKSHOP PROCEEDINGS 3

1. RECENT TRENDS IN THE USE OF THE INTERNET/ICT FOR TERRORIST PURPOSES 3

2. THE CURRENT RESPONSE 5

2.1 Emerging initiatives 5

2.2. From Policy to Action: Emerging Practices and Persistent Challenges 8

RECOMMENDATIONS 15

ANNEX I Workshop participants 18

ANNEX II Workshop Agenda 19

The views expressed in this report do not necessarily reflect those of the United Nations (UN) and the UN Counter Terrorism Committee Executive Directorate (CTED) or the ICT4Peace Foundation.

BACKGROUND

In April 2016, the UN Counter Terrorism Committee Executive Directorate (UNCTED) and the Swiss-based ICT4Peace Foundation launched a joint project on 'Private Sector Engagement in Responding to the Use of the Internet and ICT for Terrorist Purposes'. The project seeks to deepen understanding of how the private sector - notably technology and social media companies – is responding to how listed terrorist groups such as Islamic State in Iraq and Levant (ISIL) (also referred to as ISIS, IS and Daesh by workshop participants) and Al-Qaeda are using the internet and ICT for terrorist purposes in the context of a number of UN Security Council Resolutions and reports.

Within the framework of the project, it was agreed that three workshops would be held during 2016, the results of which would feed into a preliminary report to the UN Counter Terrorism Committee (CTC) in December 2016.

The first workshop was held in Zurich, Switzerland on 25 August 2016, hosted by the Swiss Federal Institute of Technology, ETH. The following report summarises the main points discussed at the workshop including trends, the policy and operational response to terrorist use of the Internet and ICT, implementation challenges, including a number of normative issues, and key recommendations. The outcome of the workshops will be incorporated into the final report to the CTC and used to shape Phase II of the project.

SUMMARY OF WORKSHOP PROCEEDINGS

1. RECENT TRENDS IN THE USE OF THE INTERNET/ICT FOR TERRORIST PURPOSES

The first of the three workshop sessions focussed on core trends in the use of the Internet and ICT for terrorist purposes. From the start of the workshop, participants were clear to distinguish between terrorists using technology to disseminate information and propaganda versus operational usage for private communications, command-and-control, or carrying out financial transactions.

In terms of terrorists publishing social media content, a participant stressed that by July 2016 the amount of original content generated by ISIL had actually fallen by more than 70 percent within six months when compared with December 2015. Such a sharp decline in the volume of digital output by ISIL was largely attributed to the "supply-side" issue of fewer active social media users posting propaganda material online due to the continued military pressure exerted in Iraq and the Syrian Arab Republic, had resulted in major

military setbacks and overall capability degradation. New content published in December 2015 was around 60 items per day, according to one workshop participant and by July 2016 this had dropped to fewer than 20 items. At the same time, grassroots counter-narrative campaigners are becoming more adept at hijacking ISIL hashtags, see for instance #isischan, or reporting accounts that appear to sympathise with terrorist groups.

According to participants, ISIL had developed a two-way communications strategy that aims to "push" and "pull" recruits through a process of deep socialisation of content by online interest communities. On this point there was discussion around the concept of radicalisation to violence and some opposition to the notion that online violent extremist content alone was enough to radicalise individuals to commit terrorist acts. A number of participants stressed that there was no significant body of evidence that suggests online content alone is sufficient to radicalise vulnerable individuals to violence.

Some workshop participants argued that terrorists acting alone and in small cells is the fastest growing type of terrorism and is also the least understood. Such attackers are heavily influenced, it was suggested, by content hosted on the Internet and curated on social networking platforms and radicalisation tends to take place in a short time within such closed virtual online communities. In the case of 700 foreign terrorist fighters (FTFs) in Syria, research by one participant has shown that for 50 percent of these the Internet played a critical role. Furthermore, 12 percent of these FTFs were found to be minors. While the Internet and social media clearly play a part in radicalising individuals, workshop participants were keen to stress that they may only play a *facilitating* rather than a *causative* role in the process.

One expert in encryption technology suggested that most technology used by terrorists in an operational capacity often hinged on unencrypted text messaging over one-time-only burner phones rather than through sophisticated technology. Despite the ubiquity of ISIL-related propaganda on social media and the Internet, operationally terrorists still tend to have a low-tech approach to carrying out acts of terrorism. For instance, the Paris attacks of 2016 demonstrated that using simple technology such as "burner phones" was as effective as sophisticated encrypted messaging.

Other participants questioned whether taking down content was counter-productive, calling for more research to evaluate the effectiveness of such policies. In response, others referenced quantitative analysis undertaken by Berger & Perez that suggests that running a sustained campaign of social media account suspensions can potentially degrade a terrorist

network.[1] Yet, terrorist users of social media are also adept at developing counter-measures such as using apps that regenerate accounts once they have been deactivated or taken down.

One participant explained that terrorist groups typically use low-tech solutions such as trading pre-paid mobile cards to source and transfer funds. Nonetheless, some experts noted an increase in the use of crowdfunding facilitated by online platforms. Furthermore, some terrorist groups are expressly marketing crypto-currencies such as BitCoin as potential platforms to help support funding their operations. The entry point for using such technologies is currently too high, however, for widespread adoption.

Participants also argued that governments could potentially use events such as the Paris terrorist attacks of November 2015 as justification for unnecessary and disproportionate surveillance programmes. In the case of the Paris terrorist attacks, the suspected chief planner and leader of the Verviers cell, Abdelhamid Abaaoud, had used Dabiq - ISIL's propaganda magazine - in January 2015 to boast about his plans to carry out a terrorist attack in Europe and then explained how he could "plan operations" and come and go as he pleased despite the fact that "[his] name and my picture have been all over the news."[3] This issue of Dabiq also included an interview with Hayat Boumeddiene, the wife of Paris kosher supermarket attacker Amedy Coulibaly[4] According to a number of workshop participants, government agencies should focus on collecting and analysing such material published by ISIL before contemplating invasive surveillance programmes. Others questioned whether intelligence and law enforcement agencies are paying enough attention to such material when evaluating potential terrorist threats.

2. THE CURRENT RESPONSE

2.1 Emerging initiatives

A number of efforts are underway globally and in Europe to respond to the use of the Internet for terrorist purposes. Major global technology and social media companies such as Microsoft, Facebook, Google, ASKfm have been engaged on these issues for some time,

[1] The Islamic State's Diminishing Returns on Twitter: How suspensions are limiting the social networks of English-speaking ISIS supporters, J. M. Berger and Helen Perez, GW Program on Extremism, Feb. 2016, retrieved from https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Berger_Occasional%20Paper.pdf

[3] What the Paris Attacks Tell Us about IS Strategy, Der Spiegel, Nov 2015, retrieved from http://www.spiegel.de/international/world/paris-attacker-abaaoud-offers-insights-into-is-strategy-a-1064902.html

[4] ISIS's English-Language Magazine 'Dabiq' Celebrates Attacks in France, Features Interview with Leader of Belgian ISIS Cell, PJMedia, Reprinting from MEMRI, retrieved from https://pjmedia.com/blog/isiss-english-language-magazine-dabiq-celebrates-attacks-in-france-features-interview-with-leader-of-belgian-isis-cell

often in response to civil society or government pressure, which is now extending to smaller companies.

In Europe, three regional bodies in particular – the European Commission (EC), the Council of Europe (CoE) and the Organisation for Security and Cooperation in Europe (OSCE) - have undertaken a number of initiatives, some in conjunction with major technology and social media companies and others in conjunction with academia and civil society organisations, to deepen understanding of the issues at hand and shape a response. Beyond Europe, non-governmental efforts such as those led by the Global Network Initiative (GNI), which brings together the major technology, social media and telecommunications companies, are also proving influential in terms of shaping or promoting principles and norms to guide private sector action in this area. The following section highlights some of these efforts.

i. The European Commission

In 2015, the European Commission established the EU Internet Forum to bring together EU Interior Ministers, high-level representatives of major Internet companies, Europol, the EU Counter Terrorism Co-ordinator and the European Parliament to counter terrorist content and hate speech online.[5] The EU Internet Forum responds to one of the key commitments made in the European Agenda on Security presented by the Commission in April 2015. More detail on how the European commission is operationalizing its response to terrorist use of the internet is detailed below.

ii. The Organization for Security and Co-operation in Europe (OSCE)

The OSCE representative at the workshop stressed that its membership is committed to developing a co-operative approach in the fight against terrorism, including the establishment, where appropriate, of public-private partnerships (PPP) between state authorities, the business community, civil society and the media. In its view, PPPs should be based on voluntary, reciprocal and trust-based collaboration between stakeholders. Over the past three years, the OSCE has organised some ten national seminars together with OSCE field operations to facilitate the exchange of good practices and lessons learnt.

Additionally, in 2015 under Serbia's Chairmanship, the OSCE Secretary General launched an Organization-wide communication campaign with the slogan 'OSCE United in Countering Violent Extremism' (#UnitedCVE).

Furthermore, the organisation is currently in the process of developing an e-learning module to provide training on Countering the Use of the Internet for Terrorist Purposes.

[5] See: http://europa.eu/rapid/press-release_IP-15-6243_en.htm

The objective of this project is to increase general awareness and knowledge on countering the use of Internet for terrorist purposes through basic knowledge and education regarding recruitment, violent radicalization and training new members, collection and transfer of funds, organization of terrorist acts and inciting terrorist violence. The expectation is that these efforts will also provide practical examples for how the OSCE and participating States could work together with civil society and business circles (through public-private partnerships - PPP), to better influence efforts relating to the use of the Internet to prevent terrorism, in full compliance with international human rights law and OSCE commitments.

iii. The Council of Europe (CoE)

The Council of Europe (CoE) representative summarised the ways in which the organisation is supporting initiatives and research programmes in this area. The presentation focused particularly on the CoE's work with respect to protecting freedom of expression online and offline [7], combating terrorism, [8] and combating cybercrime. [9] Regarding combating terrorism, work is currently underway to develop a foreign terrorist fighter (FTF) network of national contact points to strengthen timely information sharing concerning persons travelling abroad for terrorist purpose

The CoE has published a broad range of research on this matter, including a report by the Secretary General of the Council of Europe which analyses the "State of democracy, human rights and the rule of law",[10] and a comparative study, in partnership with the Swiss Institute of Comparative Law, on filtering, blocking and take-down of illegal content on the Internet. This study compares policy and practice across the organisation's 47 member States, describing and assessing both the legal framework and the relevant case-law and practice in the field and assessing the impact of those measures on freedom of expression..[11]

Additionally, the CoE has established a number of committees that focus on specific challenges. The Steering Committee on Media and Information Society (CDMSI) considers the media and issues relating to internet standards,[12] while the work of MSI-NET evaluates the roles and responsibilities of Internet intermediaries and on human rights implications

---

[7] http://www.coe.int/en/web/freedom-expression

[8] http://www.coe.int/en/web/counter-terrorism/home

[9] http://www.coe.int/en/web/cybercrime/home

[10] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680646af8

[11] See "Comparative Study on Filtering, Blocking and Take-down of Illegal Content on the Internet". Swiss Institute of Comparative Law. December 2015. Available at: http://www.coe.int/en/web/freedom-expression/study-filtering-blocking-and-take-down-of-illegal-content-on-the-internet

[12] See: http://www.coe.int/en/web/freedom-expression/cdmsi-meetings

regarding algorithms.[13] The Cloud Evidence Working Group of the Cybercrime Convention Committee (T-CY), in turn is exploring criminal justice access to evidence stored on servers in the cloud, including through mutual legal assistance. The Working Group is also developing a database that would consolidate country information on the legal situation in a given country as well as on emerging challenges regarding criminal justice access to data stored in the cloud.

iv. The Global Network Initiative (GNI)

The GNI was established to support ICT companies in light of increasing pressure by governments "to act in ways that may impact the fundamental human rights of privacy and freedom of expression". More specifically, the organisation provides a framework for companies, rooted in building trust and international standards; ensures accountability of ICT sector companies through independent assessment; enables opportunities for policy engagement; and creates shared learning opportunities between different stakeholders. The GNI representative explained how the latter has allowed the organisation develop a unique multi-stakeholder collaborative forum of ICT companies, human rights and press freedom groups, academics and investors that work to protect and advance freedom of expression and privacy in the ICT sector.[14]

2.2. From Policy to Action: Emerging Practices and Persistent Challenges

The following section highlights some of the core developments and challenges discussed during the session:

i. Definitions of terrorist use of ICT and difficulties implementing content removal guidelines

Significant emphasis was placed on the absence of an agreed definition of "terrorism" in international law, which in turn creates challenges for determining what constitutes terrorist content online. To this end, a number of global companies are using sanctions lists to inform their decisions.

The United Nations and regional organisations such as the European Union (EU) actively maintain lists of proscribed terrorist groups and individuals. Both Google and Facebook use the US terrorist list to inform their content policies, whereas Microsoft recently announced at a special meeting of the Security Council on 11 May 2016 that it would amend its terms of use – which already prohibit hate speech and advocacy of violence against others – to

[13] See: http://www.coe.int/en/web/freedom-expression/committee-of-experts-on-internet-intermediaries-msi-net-

[14] For more information, including on the GNI's annual reports, see: http://globalnetworkinitiative.org

specifically prohibit the posting of terrorist content by or in support of organizations included on the Consolidated United Nations Security Council Sanctions List in order to inform decisions relating to terrorist content. The list includes all individuals and entities subject to sanctions measures imposed by the Security Council. Inevitably, using lists of proscribed groups poses important challenges, including the risk that some governments may use such lists against political opponents or political activists, and questions relating to transparency and delisting processes and procedures. At the same time, significant effort has been made by both the UN and the EU to respond to some of these challenges. One participant stressed that the Consolidated United Nations Security Council Sanctions List is currently the only global framework that exists to inform decisions on these issues and ensure respect for the rule of law.

Workshop participants agreed that it is difficult to formulate guidelines on what content counts as "terrorist" and whether it should be taken down. The European Commission highlighted the importance of reaching out to smaller companies, particularly startups to make them aware of how terrorists could exploit their platforms. Speakers also highlighted the importance of educating users on the Terms of Service and promoting user-driven self-regulation. There was general agreement on the need to better inform the public about updates to intermediaries' Terms of Service.

Representatives from civil society stressed that symbols or indicators of terrorist content are not necessarily obvious to the layperson and therefore decisions relating to content removal require significant expertise. The case relating to Anjem Choudary in the United Kingdom shows that some individuals use their extensive knowledge of the domestic law to ensure that they can continue promoting terrorist causes while avoiding successful conviction.[15]

Some noted that when ICT companies do formulate content removal policies based on the local laws of different jurisdictions there is the concern that these can change rapidly and without warning. In this regard ICT representatives stressed the challenges of continually adapting Terms of Service to reflect political, legal and judicial developments. This is particularly challenging for for smaller internet companies that are not necessarily aware of such changes or do not have the resources to continuously revise their Terms of Service.

ii. Framework and Legitimacy of Content Removal Practices

[15] Anjem Choudary case raises terror law questions, BBC, August 2016, retrieved from http://www.bbc.co.uk/news/uk-37104446 Choudary was subsequently found guilty of supporting ISIL.

Private-sector ICT representatives stated that they had a zero-tolerance policy for terrorism on their platforms and were dedicated to ensuring the safety of their users. They stressed the importance of operating in a transparent manner in combatting terrorist content online, particularly in the context of handling and reporting government blocking and take-down requests in a manner consistent with international human rights law and standards, including the United Nations Guiding Principles on Business and Human Rights. The EU has developed a number of Sector Guides on implementing the principles, including for the ICT sector.[16]

The ICT company representatives stressed further that the people of a given country should decide what is appropriate content rather than executives at an ICT company and that international norms should shape their content policy. In this regard, speakers highlighted the importance of educating users on the Terms of Service and promoting user-driven self-regulation. There was a need to better inform the public about updates to intermediaries' Terms of Service. All ICT reps reiterated that they had a zero-tolerance policy for all forms of terrorist content or activity on their platforms. For example, the Google representative stressed that YouTube (which it owns) has an operations team dedicated to making removal decisions based on policy and this team follows a clear internal process in evaluating referrals from governments. If the legal reasoning is clear and justified, content is promptly removed.

Representatives from human rights organizations stressed that content removal practices are often opaque and that governments and technology and social media companies need to invest more in meaningful transparency rather than irregularly published reports that do not provide sufficient detail. Some participants also raised concerns that there are no open processes to ensure redress for social media users who feel that their content has been unfairly or unjustifiably removed.

iii. ***Operationalising EU content removal policy***

In 2015, the EU established an Internet Referral Unit (IRU) at Europol aimed at reducing accessibility to terrorist and violent extremist propaganda on the Internet by identifying and referring relevant online content to the hosting internet service provider, with a clear assessment of how it is terrorist material and might be in breach of their terms and conditions. Furthermore, the EU IRU supports Member States with operational and strategic analysis.[17] Since its inception, the IRU – modelled on the UK Counter Terrorism IRU - has assessed (and processed for subsequent referral to concerned Internet service

[16] See: https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/information_and_communication_technology_2.pdf

[17] See: https://www.europol.europa.eu/content/europol's-internet-referral-unit-combat-terrorist-and-violent-extremist-propaganda

providers) over 11,000 violent extremist messages across 31 online platforms in eight languages. Around 90 per cent of the content referred has been removed from the platforms by online service providers. The process is a voluntary one. It is ultimately for the companies to decide whether or not they wish to remove the terrorist content from their platform.

In terms of procedures, the IRU flags relevant operational content to the private sector either after receiving a request from a member state or through its own searches for terrorist material. All reported content goes through a human analyst or translator.

According to some participants, trust between governments and ICT companies is essential for dealing with content-related issues and it is critical for IRUs to avoid operating in grey-zones, which could lead to accusations of censorship practices. At the same time, a number of representatives from ICT companies and civil society groups questioned why governments prefer to use perceived violations of company Terms of Service over established legal norms. Concern was expressed that IRUs lack transparency and accountability because of the secrecy that often surrounds their work. In response, the Europol IRU stressed that the European Parliament and EU member states provide oversight of its work in this area, while transparency is guaranteed by its annual activity reports (the first published in July 2016, marking its first year anniversary). One civil society representative commended Europol for publishing an annual activity report, while pointing out that much remains to be done and that most IRUs are not open to such public scrutiny. Some participants highlighted the need for any reaction or process to be swift. The harm could only be mitigated if the material was taken down quickly. Any process which took days or weeks would prove nugatory due to the speed at which terrorist material was disseminated.

Other civil society representatives stressed that the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the European Convention on Human Rights and the United Nations Guiding Principles on Business and Human Rights (also referred to as “the Ruggie Principles”) should remain an important framework for any policy and operational decisions made regarding content removal.

Some participants questioned whether IRUs should be presented as a good or best practice, expressing concern that governments might increasingly use them as a means to circumvent due process and international human rights obligations through an increased dependence on these kinds of voluntary public-private partnerships.

iv. Other Public-Private Engagement Challenges

Discussions during the workshop highlighted a number of additional challenges relating to new forms of public-private engagement in response to terrorist use of the Internet and ICT.

Some participants suggested that more needs to be done to improve technical co-operation and information sharing between companies and governments to address the problem of "whack a mole." The EC stated that this was a particular concern of EU Ministers, and it was looking forward to hearing back from the companies as to how this might be addressed. In this regard some participants suggested that users should be able to flag objectionable content more easily and raised the possibility of developing a central "clearing house" for such content to improve how technology and social media companies co-ordinate content removal requests between different platforms and jurisdictions.

A representative from one ICT company stressed that there was a risk of a "one-way street" in terms of data sharing whereby governments place all of the information-sharing burden on the ICT companies. In general, workshop participants agreed that it is essential to improve information sharing between companies and governments.

v. The Mechanics of Removing Content from ICT platforms

Even if specific content has been identified and reported, most technology and social media companies generally do not support so-called "recursive takedowns" in which similar items of content are removed from across the entire ICT platform, particularly when posted by third parties. One company representative suggested that techniques from image hashing could be applied to content to help identify recursive content however there would be challenges given that content used by terrorists and their supporters is often ambiguous and sometimes re-used for legitimate reasons such as news or commentary. While content relating to child protection is usually unambiguous, journalists and researchers often reuse content used by terrorists. Furthermore, terrorist content is often intrinsically more difficult to identify algorithmically given the wider range of potential image patterns.

While all the major technology and social media companies have reportedly established dedicated take-down teams, many of these are overwhelmed by spurious reports of content violations. For example, many users report innocuous content (such as Justin Bieber videos) and in the process create noise that is difficult for the companies to filter out. Furthermore, a number of participants from large technology and social media companies stressed the unprecedented volume of content removal requests, explaining how difficult it is for their teams to analyse and act upon such a large amount of information.

Other workshop participants emphasised that content removal from websites should be considered as should access to search engines. Websites can be hosted in any country and terrorists are able to exploit this loophole to circumvent local jurisdictional oversight. An example was given of a German-language blog that was closed in Germany and then moved out of jurisdictional control into another country.

One telecommunications company representative stressed that his company does not have the legal power to access the content of communications but only the metadata in a number of restricted situations. In this regard he highlighted that telecommunications companies are much more regulated than social media/ Internet companies.

vi. Resource Constraints

During the workshop, representatives from startups emphasised that small or emerging companies are primarily focussed on growth and so often do not have the time, capabilities or resources to consider how their technologies may be used by terrorists. Some may not be aware of the broader security issues while others may not be aware that their platforms or services are being used by terrorists until law enforcement agencies come knocking at their door.

Furthermore, many startups are not large enough to have the capacity and resources to fully engage with governments or larger technology and social media companies on these issues. For instance, the nature of many startups means that a successful product with several million users can be developed and supported by just one or two individuals. Finally, in some cases start-up technology or platforms can remain fully functional even if the business behind the technology no longer exists, providing a potential challenge with regard to dealing with violations of Terms of Service.

Some start-up representatives highlighted the importance of engaging small companies on these risk issues from the out-set. Conversely, for governments and international organisations it can also be costly to identify and build relationships with startups given their high number and short lifespan. Some suggested that a longer-term approach could involve engaging with tech. universities, business schools and others – potentially even venture capitalists - to ensure a multi-disciplinary approach to the field which ensures acknowledgement of potential risks and related costs relating to ICT use from a very early stage.

vii. Unintended Consequences of Content removal

As some of the larger companies become more adept at identifying and blocking terrorist use of their products and services, there is a tendency for some terrorist users to migrate to smaller technology platforms. ISIL, however, has reportedly urged its members to

continue using mainstream social networks as it understands the advantage of having a popular platform for disseminating propaganda.

As noted above, questions abound relating to the intelligence consequences of removing terrorist-related content or accounts. This issue was raised by numerous participants during the workshop, and the question remains unresolved in most jurisdictions.

viii. The Risks of Over-Regulation

One of the workshop panels focused in part on the use of existing and emerging technology to finance terrorist activity. A representative from one of the encryption companies explained the complex identity authentication requirements it has adopted, which it believes, serves as a form of soft deterrence. Similar to other companies present at the meeting, the company also has a zero tolerance policy with regard to terrorist or any other illegal activity and cooperates fully with law enforcement agencies. Its system architecture also provides two technical options in connection with legally authorized, official investigations: (i) provision of metadata on the communication activity of a client's users; and (ii) shutting down the service for some or all of the users of the client who is under the terrorist investigation.

Workshop participants also discussed the downside of "over-regulation". In this regard, a representative from one trade body representing electronic money transfers stressed that regulations designed to increase the Know Your Customer ("KYC") threshold could have significant impact on legitimate users who could ultimately end up "unbanked". The effect of this could lead to an increase in the so-called "shadow economy" by promoting cash transactions as well as an increase in transaction costs for the remaining financial transactions users. It was suggested that more onerous KYC authentication processes could cost as much as €5-10 per new customer.

ix. Counter Narrative Challenges

While the meeting did not specifically focus on the topic of strategic communications and countering the narratives of groups such as ISIL, one civil society representative discussed new research that demonstrates the limited impact of many of the largest publically-funded counter-narrative initiatives in the Middle East and North Africa region. In many cases the general population had not heard of them and whenever such initiatives are associated with CVE, they then develop a negative reputation.[19] Acknowledging some of

[19] See, for example, the work of the Global Forum for Media Development on this subject: http://gfmd.info/en/site/news/957/GFMD-Workshop-"Mediadev-CVE--counter-propaganda-Where-is-the-problem"-Brussels-Press-Club-26-April-2016.htm. See also Ferguson, Kate (2016) Countering violent extremism through media and communication strategies: A review of the evidence http://www.paccsresearch.org.uk/wp-content/uploads/2016/03/Countering-Violent-Extremism-Through-Media-and-Communication-Strategies-.pdf

these challenges in policy and practice is all the more important given a number of organisations including the UN and the Global Counter Terrorism Forum (GCTF) are launching a number of initiatives in this area.

Separately, the European Commission stated that an important objective of the EU Internet Forum was to empower civil society partners within the EU to provide positive alternative narratives online. These credible voices often lacked the necessary technical support or expertise to be able to produce effective narratives online. The Commission had therefore committed €10 million to support civil society partners in this way.

RECOMMENDATIONS

Recommendations for next steps focused on a number of mechanisms and platforms for sharing knowledge, information, exchange of practices and capacity building. These could possibly be combined under one comprehensive initiative.

i. *Knowledge Sharing Platform for Content Management-related Initiatives*

Participants stressed the need for a curated public-private platform that could help a range of stakeholders keep abreast of ongoing initiatives (such as the Global Network Initiative) and the numerous research programmes currently underway in this area. In more concrete terms, such a resource could also provide a detailed list of relevant contacts at technology and social media companies and help governments navigate technology and social media company's content management policies, processes, and expectations. It would provide a "one-stop shop" for learning about the principles, norms and practices underpinning both the government and company response to terrorist content online, with samples of good practice regarding Terms of Service, legislation and related information. The challenge with such a platform would be to ensure that the information was regularly updated as both Terms of Service and government practice change frequently.

Others suggested that as a means to deepen understanding and assess the effectiveness of current company practices, a number of indicators could be assessed across a sample of companies. These could include:

- The average time lapse between the moment terrorist-related content is published and subsequently removed.
- The average reach of the material (in terms of views/users).
- The average time it takes to review the material.

- The rate at which the same material is published (e.g. propagation of the same video).
- Most common methods employed to search for terrorist-related content (trusted flaggers, users etc.).
- The technological solutions currently being used to support ICT companies identify terrorist content.
- Whether companies report terrorists content directly to law enforcement - and how often the same report is repeated.

One global company representative suggested the possibility of accelerating work on a concept they are currently discussing with other industry actors involving the creation of a back-office "clearing house" for terrorist content. Such an initiative would help facilitate knowledge-sharing between different technology and social media companies and avoid duplication of effort by users/IRUs reporting content, and companies removing it.

ii. Capacity Building for the Tech Sector

Related to the point, significant emphasis was placed on the importance of capacity building efforts in this area, ultimately supported by a curated global knowledge-sharing platform. Complementing existing initiatives such as the GNI, the platform could include a "Startup Toolbox" that includes pragmatic advice and detailed information on existing good practices, international principles and norms, and additional resources. In this regard, participants emphasised the usefulness of a knowledge-sharing platform that could provide guidance to private sector startups and small Internet intermediaries to develop their Terms of Service and user policies, particularly in the context of addressing content removal requests and effectively monitoring and responding to potential use of their products and services by terrorists in a manner consistent with international human rights law and standards, including the United Nations Guiding Principles on Business and Human Rights.

As part of building this platform, participants highlighted the need to engage directly with small companies, including startups, for instance through holding a series of small workshops at tech hubs and incubators around the world. They also stressed the importance of learning *how* to engage with small companies and startups and not just developing material to support their efforts against terrorist use of their technologies. This would require much more in-depth work with a number of sectors, including trade associations, business and law schools as well as new and emerging businesses. Furthermore, given low levels of awareness of the issues, many new companies may require more information on the potential risks of terrorist exploitation of the Internet and ICT. Several suggestions were put forward on how to leverage existing cyber security capacity building tools and platforms to such ends, the importance of engaging universities across a range of disciplines (technology, business, law).

iii. Make it easier for the public to report harmful terrorist material

While there are some strong approaches to crowdsourcing reporting of terrorist material in some countries, participants felt that practice is uneven and that this group should determine ways to develop a more unified approach to encouraging the public to report content to ICT via a single reporting platform. Furthermore, a number of participants mentioned the possibility of helping inform users on expectations of take-down turnaround times or delving deeper into the due process challenges relating to legitimising content removal requests.

iv. Research future risk of terrorist use of internet technologies

Workshop participants suggested that a separate research programme was required to investigate future potential uses of Internet / ICT technologies for terrorist purposes.

v. Promote understanding of requirements for effective public-private partnerships

Participants spoke of the need help governments and technology and social media companies develop two-way partnerships and called for new research into the role of public-private partnerships in this area. Contributors also pointed out that non-Western governments often found it more difficult to engage with Western technology companies, suggesting that this should be one area of focus of the workshop organisers. Civil society groups reiterated the need to ensure that all governments are aware of their obligations to safeguard human rights when engaging in PPPs.

vi. Develop a knowledge-sharing platform of global counter-narrative programmes

Participants suggested the need for an international organisation such as the UN to host (and regularly update) information on global counter-narrative programmes, including research into their effectiveness.

ANNEX 1 Workshop participants & Project Team

Participants

Council of Europe, CryptTalk, Dublin City University/VoxPol, Electronic Frontier Finland, Electronic Money Association, Embassy of Spain, Government of Switzerland, ETH, European Commission, EUROPOL IRU, Facebook, FSM, GCERF, GNI, Google, Gov. of Switzerland, Gov. of UK/Home Office, ICT4Peace, KASPERSKY LAB, KPMG, Kudelski Group, LaQuadratureduNet, Martin School/University of Oxford, Microsoft, Moonshot CVE, Open Net Initiative, Open Systems AG, Orange, OSCE, Pretty Easy Privacy, Samir Kassir Foundation, SECDEV Foundation, Telefonica, Treasure My Text, Twoo / Massive Media, UBS, UN CTED, UN ISIL/ AQ Monitoring Team, UN OHCHR, UN OICT, UNICRI , VoxPol, WEF.

Project Team

Joint project directors:

Camino Kavanagh (ICT4Peace) and Marc Porret (UNCTED)

Project researchers/ associates:

Adam Hadley (Zurich lead/ report drafter), Sophia Khan,

Diana Ruiz (ICT4Peace)

Matteo Sestito and Katie (UNCTED)

CTED Counter-Terrorism Committee Executive Directorate

ICT for peace foundation

Annex II Workshop Agenda

THURSDAY, 25 AUGUST 2016		
09:00 - 09:30	**WELCOME & INTRODUCTORY REMARKS**	
		Introduction Dr. Camino Kavanagh, ICT4Peace - Mr. Dirk Helbing, ETH - Amb. Stephan Husy, Amb. at large for Counterterrorism, Government of Switzerland - Mr. JP Laborde, Assistant Secretary-General and Executive Director, UN CTED - Amb. (ret.d) Daniel Stauffacher, Pres. ICT4Peace
09:30 -10:30	**SESSION 1** **FRAMING THE MEETING**	
	Terrorism and the internet/ ICT: overview of current trends	***Speakers*** - Dr. Maura Conway, DCU - Mr. Alex Corbeil, SecDev Foundation - Mr. Volker Birk, PeP
10:30 - 11:30	**TERRORISM, ICT & THE INTERNATIONAL AND REGIONAL POLICY RESPONSE**	
	Developments in the UN Security Council relating to use of the internet/ICT for terrorist purposes. Developments in the European Union Developments in the Council of Europe	***Moderator*** Dr. Myriam Dunn-Cavelty, ETH ***Speakers*** - Mr. Marc Porret, UNCTED Mr. Xu Yu, UN ISIL-AQ Sanctions Monitoring Team - Ms. Lucinda Armstrong, EU Home & Migration Affairs - Ms. Silvia Grundmann, Council of Europe

11:30 - 13:00	**SESSION 2** **STANDARDS, PRINCIPLES & PRACTICES UNDERPINNING THE INDUSTRY RESPONSE**	
	Industry response to use of internet/ ICT products and services for terrorist purposes. Emerging trends (standards, principles and practices) relating to content management/ Identification of challenges (business, legal/jurisdictional, political, technical, human rights etc.).	***Moderator*** Prof. Paul Cornish, RAND/Oxford U. ***Speakers*** - Mr. Steve Crown, Microsoft - Mr. Peter Stern, Facebook - Ms. Brittany Smith, Google - Mr. M.Reveyrand-de Menthon, Orange - Mr. Attilia Matrenyi, Crypt Talk - Mr. Javier Ruiz, Open Rights Group & Ms. Agnes de Cornulier, laQuadratureduNet.

14:30 - 16:00	**SESSION 3** **STANDARDS, PRINCIPLES & PRACTICES UNDERPINNING PUBLIC-PRIVATE ENGAGEMENT**	
	The normative framework underpinning relations between law enforcement and industry for content management The nature of existing and emerging public-private initiatives Assessing the impacts and effectiveness of existing efforts.	***Moderator*** Mr. Marc Porret, UNCTED ***Speakers*** - Mr. Jan Neutze, Microsoft - Mr. Stephane Duguin, EUROPOL IRU - Ms. Ushang Damachi, World Economic Forum - Ms. Sarah Saft, FSM - Mr. Mark Stephens, Independent Chair, The Global Network Initiative (GNI)

16:00 – 17:00	**SESSION 4** **ADAPTING TO FUTURE CHALLENGES**	
	Beyond AQ and ISIS: Adapting to emerging and future digital terrorist threats	***Moderator*** Mr. David Stokar, KPMG ***Speakers*** - Mr. Thaer **Sabri**, Electronic Money Association - Mr. Jim Hales, UBS - Mr. Anton Shingarev, Kaspersky Lab - Mr. André Kudelski, Kudelski Group - Mr. Miguel Sanchez, Telefonica
17:00 – 18:00	**SESSION 5**	***Facilitator*** Mr. Adam Hadley, ICT4Peace
	Open Discussion: Establishing a Global Collaboration Forum	